Peter C. Hildreth
Bank Commissioner

Robert A. Fleury
Deputy Bank Commissioner

64B Old Suncook Road
Concord, NH 03301

Phone (603) 271-3561

Division FAX Numbers:
Banking (603) 271-1090
Consumer Credit (603) 271-0750

The
BANKING DEPARTMENT NEWSLETTER
SPRING 2004

www.state.nh.us/banking Volume 3 • Issue 2

Carolyn L. Bond, *Assistant to the Commissioner*

Note from the Commissioner

I use this space to highlight information that is important to our regulated industries. However, this time I have information that I am not pleased to be announcing.

Carolyn Bond, Assistant to the Commissioner, will retire effective June 30, 2004. Although still a young woman, Carolyn has been with the Banking Department for 28 years. In total, she has been a state employee for over 37 years. To put things into perspective, when she went to work for the State of New Hampshire, Lyndon Johnson was President of the United States and John King was Governor of New Hampshire.

Now, I have only known Carolyn for 2 ½ years. But, she has been the institutional memory that I have relied upon for all of my tenure as Bank Commissioner. I used to joke that she could only retire when technology has advanced to the point where we could download the data in her brain to run on our computer system. Unfortunately for me, she has decided to retire now.

I know that no person is indispensable. But, I also know that she leaves big shoes to fill. All of us – the employees of the Banking Department, state employees from other departments and all of our regulated entities – will miss her. I am sure we all wish her well in her retirement years.

BANKING DIVISION NEWS

Charles M. O'Connor – Chief Bank Examiner

FYI

Phishing costs American consumers and businesses billions of dollars each year, and a new government report covers how to detect, prevent and mitigate the effects of this Internet scam. The report found that the websites of the financial services industry were the most commonly spoofed. Some of the prevention steps recommended in the government report included: personalizing e-mails to customers so that they know they are legitimate; keeping website certificates up to date; and providing telephone numbers on websites where customers may verify e-mail requests for information. The report may be found online at **http://www.treas.gov/offices/domestic-finance/financial-institution/cip/pdf/fbiic-fsscc-report-2004.pdf**

Director and Officer Resources

The following web-sites are good sources of information for directors and others within the institution:

http://www.fdic.gov/regulations/resources/directorscorner/index.html

The FDIC Director's Corner offers guidance for insured institutions and their officers and directors to use to fulfill their responsibilities.

http://www.fdic.gov/bank/analytical/stateprofile/index.html

Banking and economic conditions described for each state, listed by FDIC region.

http://www2.fdic.gov/sdi/index.asp

Statistical information is available through this website.

Fidelity Bond Coverage

Financial institution fidelity bond insurance coverage is becoming increasingly important in today's banking environment. As institutions grow in size, products, and services, management needs to ensure that the fidelity bond coverage is commensurate with the risk profile of the institution. Adequate coverage is necessary in order to help protect the viability and integrity of the institution.

Fidelity bond coverage is required for each institution under the supervision of the commissioner, as detailed in NH RSA 383:14. The bonds provide for the protection or indemnity against losses from dishonest or criminal acts of officers, employees, and agents of the institution, and acts of burglary, or forgery by persons not associated with the institution. Subsequently, the commissioner has adopted a series of NH Administrative Rules in Ban 1104 pertaining to fidelity coverage requirements. Management should refer to this rule when assessing the adequacy of the institution's fidelity coverage.

Generally, the board of directors or trustees of a bank is responsible for determining the amount of fidelity bond coverage. Areas to consider include, but not limited to, the internal auditing safeguards employed; number of employees; amount of deposit liabilities; and the amount of cash and securities normally held by the bank. The fidelity bond must cover each officer, employee, and agent who has control over or access to cash, securities, or

other property of the institution; or, is actively concerned in the administration of the institution. Fidelity coverage for non-depository trust companies follows similar guidance as banks; however, management must take the fiduciary business risk into consideration when determining adequacy. Credit union fidelity coverage is based on total assets. Credit union management should refer to Ban 1104.05 when determining insurance adequacy.

A comprehensive review of fidelity bond coverage needs to be conducted annually. Ban 1104.08 details the requirements for the board of directors or trustees to review the adequacy of coverage in relation to the risk exposure of the institution. An evaluation of the institution's internal controls should be done in conjunction with the fidelity coverage review.

Violation of the Bank Secrecy Act:

Too high of a cost for both financial institutions and national security

FinCEN is one of the Government's primary agencies to oversee and implement policies to prevent and detect money laundering and other financial crimes. It is organized to network governments, people and information in support of both the law enforcement and intelligence communities. This dynamic network links the law enforcement, financial and regulatory communities domestically and internationally together for the common purpose of preventing, detecting, and prosecuting financial crime.

FinCEN works to accomplish this mission in three ways. First, as administrator of the Bank Secrecy Act (BSA), our nation's comprehensive anti-money laundering statute, FinCEN obtains certain data from financial institutions. The law's record keeping and reporting requirements help establish a financial trail for law enforcement to follow as they track criminals, their activities, and their assets. Second, FinCEN's intelligence analysts utilize the information collected to uncover leads and hidden pieces of the puzzles contained in money laundering schemes that can be highly convoluted as well as global in scope. BSA information, especially suspicious activity reports (SARs), play an important role in the success of an investigation and/or prosecution of criminal activity. And finally, this valuable information is disseminated to the law enforcement, intelligence, regulatory and financial communities.

The most prevalent type of suspicious activity is structuring. Structuring occurs when a person engages in multiple cash transactions divided into amounts low enough to avoid the filing of a CTR or other BSA reporting or record keeping requirements. Structuring can take two basic forms. A person can structure by engaging in multiple transactions on a single day through the same or several branches or can also structure by engaging in multiple transactions through the same branch or different branches over a period of days. Even apparently isolated instances of structuring can be part of a larger pattern of transactions involving several individuals and financial institutions. While each financial institution would see only one or two suspicious transactions, SARs filed by all financial institutions enable law enforcement to see a scheme that stretches across multiple financial institutions.

In order to effectively administer the BSA, FinCEN relies on regulatory agencies. Each financial regulator is responsible for the examination of its financial institutions regarding compliance with the BSA. Non-compliant institutions may be referred to FinCEN for enforcement action in appropriate circumstances. The main objective of FinCEN's enforcement policy is to gain compliance by issuing guidance. While the vast majority is in compliance; the objective for those whose programs are not in compliance is to assist them in correcting their violations as well as to ensure that the required records and reports are made available to law enforcement. When FinCEN issues warning letters, it is meant to produce effective remedial actions. Punitive action such as civil money penalties are reserved for cases involving only serious and repeated – or in the term of the statute – willful violations.

Civil money penalties assessed as a result of regulatory enforcement actions have ranged from $100,000 to $26.1 million. A listing of regulatory enforcement actions can be found at **www.fincen.gov/reg_enforcement.html**. A useful exercise for all BSA officers would be to review the enforcement actions to identify the types of offenses that result in these significant civil money penalties. It could be surprising.

Recognizing the value and the necessity of the Bank Secrecy Act in our nation's fight against financial crime is imperative. BSA officers must ensure that their institution's BSA program is not only comprehensive, but effective. The Bank Secrecy Act is one of primary regulatory concern. BSA officers should continually review their programs to avoid potential violations and the assessment of civil money penalties.

Check 21

The Check 21 Act was signed into law on October 28, 2003 and will take effect on October 28, 2004. Although the Check 21 Act does not require any "bank" (defined by the Check 21 Act to include insured banks, savings banks, credit unions and savings associations) to create substitute checks or to accept checks electronically, it does require banks to accept a legally equivalent substitute check in place of an original check after the Check 21 Act's effective date of October 28, 2004. Accordingly, banks should begin planning for operational changes needed to implement the Check 21 Act.

The Act requires each bank to provide its customers with a notice that describes substitute checks and the rights consumers have when they receive substitute checks. This notice must be sent to customers who receive original or substitute checks with the bank's first "regularly scheduled communication" after the Check 21 Act becomes effective on October 28, 2004. For new account holders, the notice must be provided to consumers who later receive substitute checks in response to requests for copies of checks. *(Source: Michael Zamorski, FDIC, May 2004)*

The Independent Community Bankers of America have available for purchase a communication tool for alerting customers about the upcoming changes in check processing. It provides information in a simple format that educates consumers about the Check 21 Act, substitute checks, and legal rights under the new law. Orders or requests for additional information may be faxed to the ICBA at (320) 352-5766.

Counterfeit Cashier's Checks

The Banking Department has received several inquiries from bank customers regarding counterfeit cashier's checks. Bank customers who deposited the counterfeit checks in their bank accounts expressed a lack of understanding that the funds were provisional and subject to set-off in the event that the check was counterfeit. A statement by bank tellers made at the time of deposit carefully explaining that the funds are subject to numerous conditions and should not be relied upon as safe would go a long way to solving this problem.

CONSUMER CREDIT DIVISION NEWS

Mary L. Jurta – Director of Consumer Credit

House Bill 1320 was signed by Governor Benson on May 24, 2004 and becomes effective on July 23, 2004. The department would like to point out some areas of this law that may apply to your business. Most of the provisions apply to all licensed companies and simply make clear routine requirements such as licensees must keep accurate books and records, must abide by federal laws and rules applicable to their business, and must supervise their employees, agents and branch offices.

Effective July 23, 2004, anyone who makes or brokers second mortgage loans on New Hampshire residential property must obtain a second mortgage license. Prior to that date, the person had to expect remuneration, directly or indirectly in order to be required to be licensed. The companies making the loans always expected remuneration in the form of interest, so there is really nothing new for second mortgage home loan lenders; they always had to be licensed. But now everyone who arranges (brokers) for the second mortgage loan, even as a courtesy or convenience without remuneration, must obtain a New Hampshire second mortgage broker license. As in the past, when a company already holds a first mortgage license, only a simple notice need be filed. The notice can be obtained at our website at www.nh.gov/banking.

One provision is specific to persons licensed as second mortgage home loan lenders who are not also licensed under the first mortgage statute. Companies who hold only a second mortgage home loan lender license have always been required to have $25,000 cash available at each licensed location (or $25,000 invested in loans at each location). The new provision allows such a company an option to post a single surety bond in the amount of $25,000 in place of meeting the cash requirement.

Two provisions apply specifically to small loan lenders. They have the same $25,000 per location requirement as second mortgage home loan lenders. Small loan lenders now may also post a single $25,000 surety bond in lieu of compliance with the $25,000 cash requirement. The second provision affecting small loan lenders applies only to title loan lenders and payday loan lenders. Such lenders are required to have a physical business location in New Hampshire where consumers can go to conduct business.

As always, please feel free to call the Licensing Section at 271-8675 with any questions.

Is It a Branch Office?

Many licensees utilize retail space in different businesses. Often, mortgage companies will have a desk and a place to meet with consumers within Real Estate Offices. If your company avails itself through this type of marketing, please be sure that location is licensed as a branch. Branch office applications are available on the department's website or by contacting the licensing section of the Consumer Credit Division at 271-8675 to have an application mailed to you.

If you are unsure if your location requires a license, please contact Celeste or Andrea at 271-3561.

When To File An Authorization/Release Form And A Personal Financial Disclosure?

There are always questions that arise regarding when and why the *Authorization/Release Form* ("Authorization") and *Personal Financial Disclosure Statement* ("PFD") must be filed. Failure to file these documents can result in delays in approval of applications for new companies, branches and/or changes in ownership. There are also particular omissions that we see repeatedly on the PFDs. We hope this article will answer some questions and assist in properly completing the form(s).

New Applications

The *Ownership and Management* section requires a new applicant to list "…all names, business and residence addresses and titles of the applicant's **principal shareholders (10% or more), officers**, ...**senior managers**...**and directors of a corporate applicant; the general partners of a general partnership; the general and limited partners of a limited partnership; the members of a limited liability company; or the trustees of a business trust…**[emphasis added]…"

What we often see is that applicants will list the "…principal shareholders (10% or more)…" but omit everyone else. The ownership and management information must list *any of the aforementioned individuals who* are part of the applicant's organization. For example, if the sole shareholder (100%) is the president of the company, but there is also a vice-president, a secretary and a treasurer who are not shareholders, they, too, must be listed on the application. Accordingly, Resumes, Authorizations and PFDs must be filed for each individual.

Branch Managers

It is necessary to submit a resume, authorization, and a PFD for a branch manager when either a branch office is being licensed at the same time as the principal, or subsequent to, or if a new manager is being appointed at an existing NH branch. Publicly-traded companies, their subsidiaries, direct subsidiaries, affiliates of an institution whose deposits are insured by any agency of the federal government need only to notify us of changes in their branch managers and submit a resume for the new manager. Authorizations and PFDs are not required.

Additions of or Changes in Officers or Directors, Managers, Members, Partners, Changes in Ownership, or Control

An Authorization and PFD must be submitted whenever a licensee changes or adds a new officer, director, manager, member, partner, trustee or owner of 10% or more, unless the company is publicly traded or a subsidiary thereof or a direct subsidiary or affiliate of an institution whose deposits are insured by any agency of the federal government.

The Personal Financial Disclosure Statement and Personal Balance Sheet

We see recurring omissions on the PFD. On the Personal Balance Sheet, certain asset categories request submission of a "schedule with details." These schedules should give further details as to what comprises the total figure for the item for which it is requested (e.g. marketable securities, real estate, other assets).

The other omission we often see on the Personal Balance Sheet is that of the individual's net worth in the business. The simplest example is if one individual is 100% owner of a business, another is a 50% owner and another is a 33% owner, and the net worth shown on all three of the companies balance sheets is $100,000, then the figure that should be entered on the Personal Balance Sheet under "Net Worth of Business" would be $100,000, $50,000 and $33,000, respectively.

A related item on the Personal Balance Sheet is found in question 4A which is the amount of an individual's current investment (for an established business) or the amount to be invested (if a start-up business and no investment has been made at the time of application). An investment in the business would be the actual cash or actual cost of goods and property that an individual contributes to a business. The figure to be entered in question 4A is calculated as the percentage of ownership times

the net worth shown on the company's current balance sheet. Depending on many factors, the resulting figure could be more or less than the individual's initial investment. For example, if an individual is a 50% owner of a business, and $10,000 is initially invested, factoring in subsequent income and/or expenses, the net worth of the business as of the date the balance sheet is prepared becomes $6,000. Accordingly, the amount of the individual's *current* investment in the business will be $3,000 which will represent 50% of the business.

If the business is a start-up, the amount of the initial investment is $10,000; the individual is 100% owner; and the company's balance sheet shows initial office expenses of $1,500, the net worth of the business at start-up then becomes $8,500. The applicant would enter $8,500 in response to question 4A which will represent 100% of the business.

As always, you may contact us at 603-271-8675 with any questions you may have.

New Hampshire BAN 2407.02: Notice of Significant Events

New Hampshire BAN 2407.02 requires all licensees to notify the Department of the occurrence of "significant events". It has recently come to the Department's attention that some licensees may not be aware of this requirement. Failure to notify the Department of a significant event is a violation of New Hampshire law that may trigger an enforcement action. A letter summarizing the significant event submitted to the Department by an officer or director is sufficient to meet this requirement. Notices should be sent to the department (Attn: Licensing).

Two different time frames are set forth in the code depending on the type of event. Both require immediate notice. This can be accomplished by a simple phone call or fax. (Send faxes to 603-271-7050 ATTN: Licensing). Notification in writing is also required. Some events are significant enough that written notification is required within one day of the event. Examples of "Significant events" subject to this time frame are:

- filing for bankruptcy;
- reorganization of the licensee;
- the filing of any information accusing the licensee of a crime or indictment related to lending activities, receiving notification of a license denial, cease and desist for any other formal administrative action in any state based on the lender or brokering activities; and
- expiration of lines of credit (for any reason).

In other instances the Licensee must notify the banking department immediately, and in writing within five business days of certain occurrences. These occurrences are (please note this is not an all inclusive list):

- filing for bankruptcy of any of the licensee's officers, directors, or affiliates;
- criminal felony indictment or conviction of any of a licensee's officers, directors, affiliates or owners of 10% or more of the licensee's stock; and
- filing of a civil suit (except small claims actions) naming licensee as a defendant which is related in any way to the mortgage lending or brokering activities.

If you are unfamiliar with this provision, please review BAN 2407.02. Or if an event occurs and you are unsure as to if you are required to report such event, please give the Department a call and we are happy to assist you in making that determination. 603-271-3561, ask for Andrea Boudreau, Esq.

Gramm-Leach-Bliley Act ("the Act"), Financial Privacy and FTC Rules

(This information has been extracted, paraphrased and summarized by the NH Banking Department from the FTC's website; please visit the FTC's websites for complete and comprehensive information about how to comply with the Act)

Any financial institution that provides financial products or services to consumers must comply with the privacy provisions of Subtitle A of Title V of the Gramm-Leach-Bliley Act ("GLB Act") (codified at 15 U.S.C. §§ 6801-09). Companies such as small loan lenders (including payday and title loan lenders), mortgage lenders, mortgage brokers, mortgage servicing companies, sales finance companies and debt adjusters that are licensed by the New Hampshire Banking Department ("licensees") must comply with the Federal Trade Commission's Privacy Rule and its Safeguards Rule which were implemented to ensure compliance with the GLB Act.

Licensees have responsibilities under the FTC's Privacy Rule regardless of their size, affiliate relationships, or information collection and disclosure practices. The Privacy Rule is focused not only on regulating the disclosure of financial information about customers and consumers, but also on requiring each financial institution to provide initial and annual notices of its policies to its customers. Please see the FTC's website at **www.ftc.gov/privacy/glbact** for information about your company's obligations to provide notices to customers and consumers.

Licensees also have responsibilities under the FTC's Safeguards Rule. Many licensed companies collect personal information from their customers, such as their names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Gramm-Leach-Bliley (GLB) Act and the FTC's Safeguards Rule require financial institutions to ensure the security and confidentiality of this type of information.

The Safeguards Rule requires licensees to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the licensee's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each licensed company must:

1. designate one or more employees to coordinate the safeguards;
2. identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
3. design and implement a safeguards program, and regularly monitor and test it;
4. select appropriate service providers and contract with them to implement safeguards; and
5. evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

These requirements are designed to be flexible to allow each licensee to implement safeguards appropriate to its own circumstances. For example, some licensees may choose to describe their safeguards programs in a single document, while others may memorialize their plans in several different documents, such as one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate safeguards or may spread this responsibility among several employees who will work together.

In addition, a firm with a small staff may design and implement a more limited employee training program than a firm with a large number of employees. And a licensee that doesn't receive or store

any information online may take fewer steps to assess risks to its computers than a firm that routinely conducts business online.

When a firm implements safeguards, the Safeguards Rule requires it to consider all areas of its operation, including three areas that are particularly important to information security: employee management and training; information systems; and managing system failures. Firms should consider implementing the following practices in these areas. The success or failure of a company's information security plan depends largely on the employees who implement it. Some suggestions the FTC offers are to:

Employee Management and Training

1. Check references prior to hiring employees who will have access to customer information.
2. Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.
3. Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
   - locking rooms and file cabinets where paper records are kept;
   - using password-activated screensavers;
   - using strong passwords (at least eight characters long);
   - changing passwords periodically, and not posting passwords near employees' computers;
   - encrypting sensitive customer information when it is transmitted electronically over networks or stored online;
   - referring calls or other requests for customer information to designated individuals who have had safeguards training; and
   - recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.
4. Instruct and regularly remind all employees of your organization's policy - and the legal requirement - to keep customer information secure and confidential. You may want to provide employees with a detailed description of the kind of customer information you handle (name, address, account number, and any other relevant information) and post reminders about their responsibility for security in areas where such information is stored - in file rooms, for example.
5. Limit access to customer information to employees who have a business reason for seeing it. For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent they need it to do their job.
6. Impose disciplinary measures for any breaches.

Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. The FTC offers some suggestions on how to maintain security throughout the life cycle of customer information - that is, from data entry to data disposal:

1. Store records in a secure area. Make sure only authorized employees have access to the area. For example:
   - store paper records in a room, cabinet, or other container that is locked when unattended;
   - ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;
   - store electronic customer information on a secure server that is accessible only with a password - or has other security protections - and is kept in a physically-secure area;
   - don't store sensitive customer data on a machine with an Internet connection; and
   - maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.
2. Provide for secure data transmission (with clear instructions and simple security tools) when customer information is collected or transmitted. For example:
   - if you collect credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit;
   - if you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail; and
   - if you must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.
3. Dispose of customer information in a secure manner. For example:
   - hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;
   - shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up;
   - erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information;
   - effectively destroy the hardware; and
   - promptly dispose of outdated customer information.
4. Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. For example, supplement each of your customer lists with at least one entry (such as an account number or address) that you control, and monitor use of this entry to detect all unauthorized contacts or charges.
5. Maintain a close inventory of your computers.

Managing System Failures

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. The FTC offers the following suggestions:

1. Maintain up-to-date and appropriate programs and controls by:
   - following a written contingency plan to address any breaches of your physical, administrative or technical safeguards;
   - checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
   - using anti-virus software that updates automatically;
   - maintaining up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations; and
   - providing central management of security tools for your employees and passing along updates about any security risks or breaches.
2. Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. For example, back up all customer data regularly.
3. Maintain systems and procedures to ensure that access to nonpublic consumer information is granted only to legitimate and valid users. For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with the licensee electronically.
4. Notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access. Please visit the FTC's websites at **www.ftc.gov/privacy/glbact and www.ftc.gov/infosecurity** for more information.

State of New Hampshire
BANKING DEPARTMENT
64B Old Suncook Road
Concord, NH 03301

New Hampshire Banking Department Newsletter

SPRING 2004